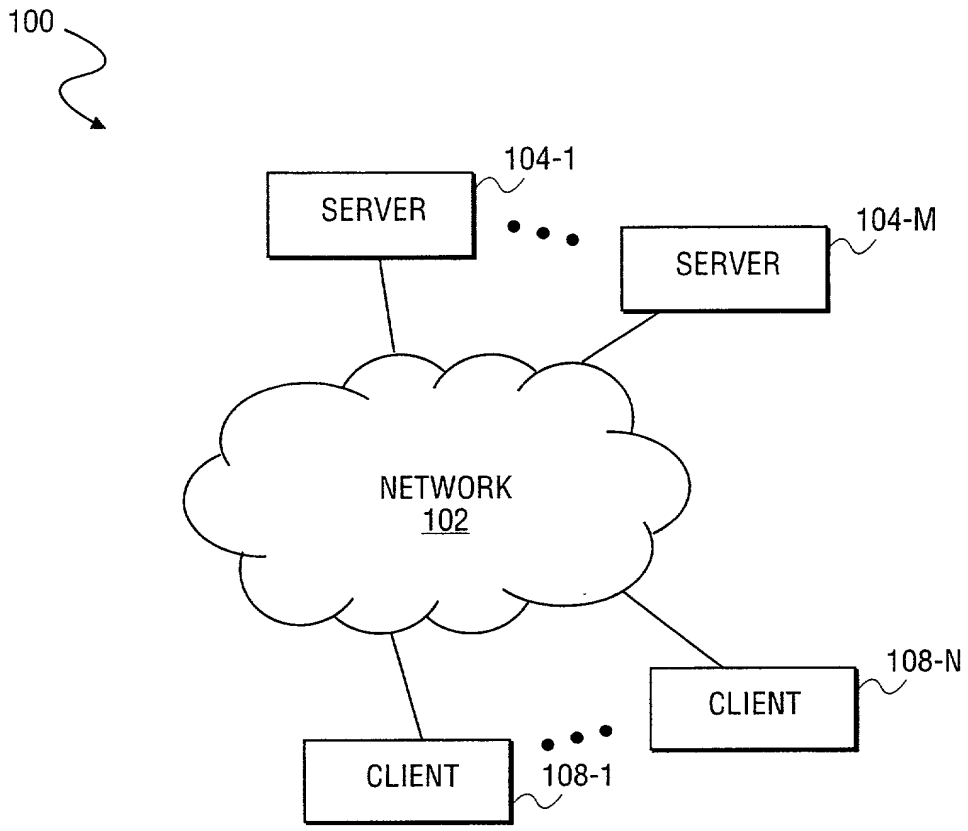
100
104-1
SERVER
104-M
SERVER
NETWORK
102
108-N
CLIENT
CLIENT
108-1

FIG. 1

Microsoft Internet

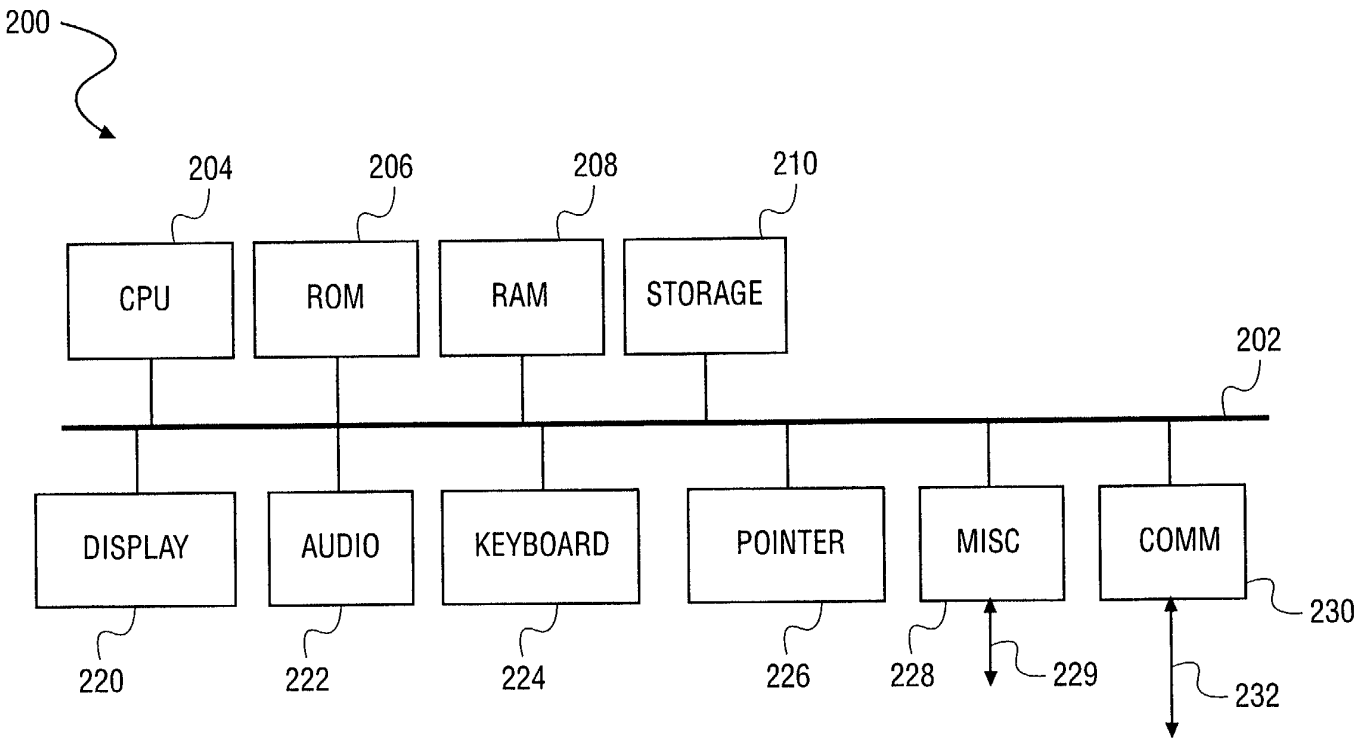

FIG. 2

Patent Application

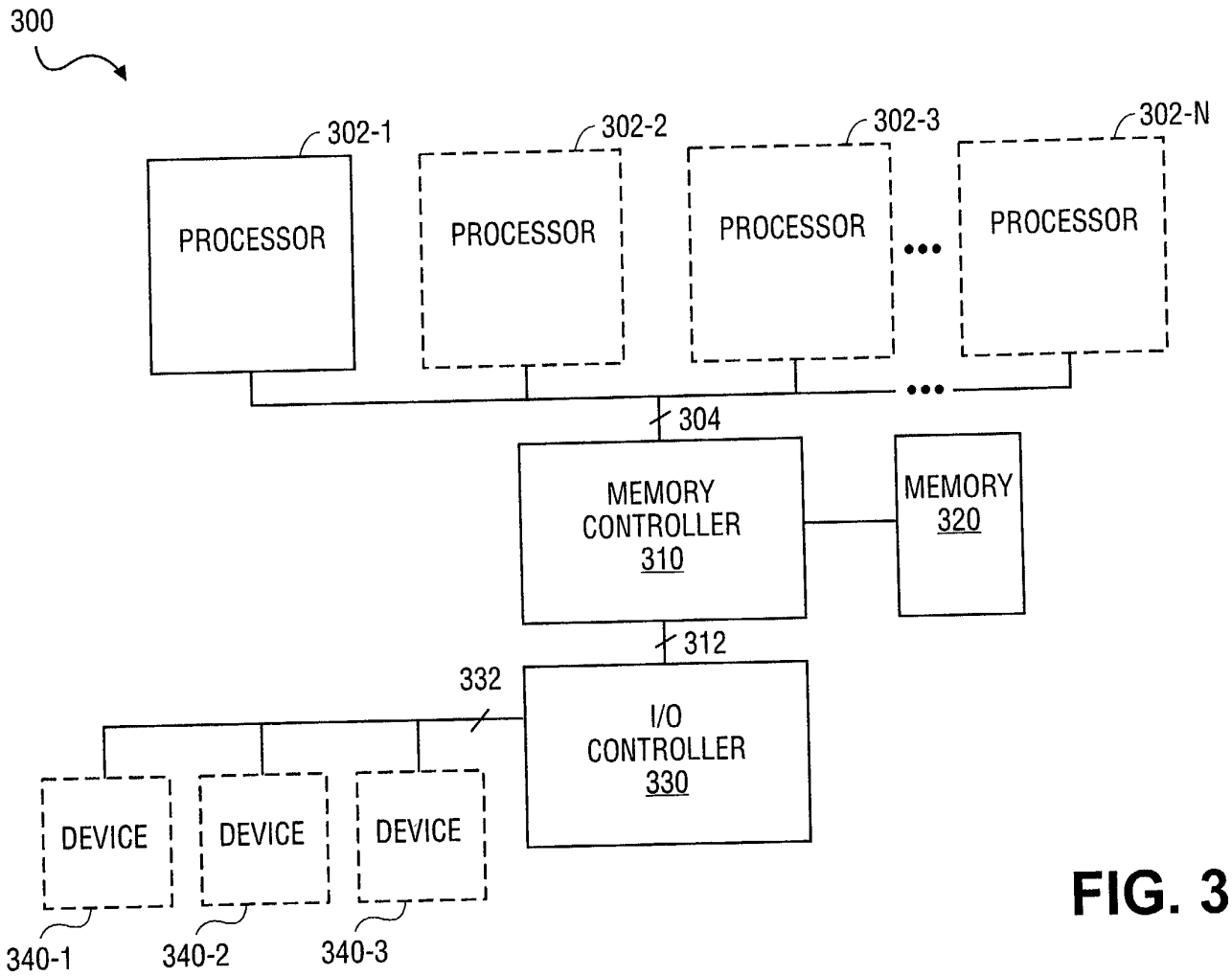

FIG. 3

Patent Application

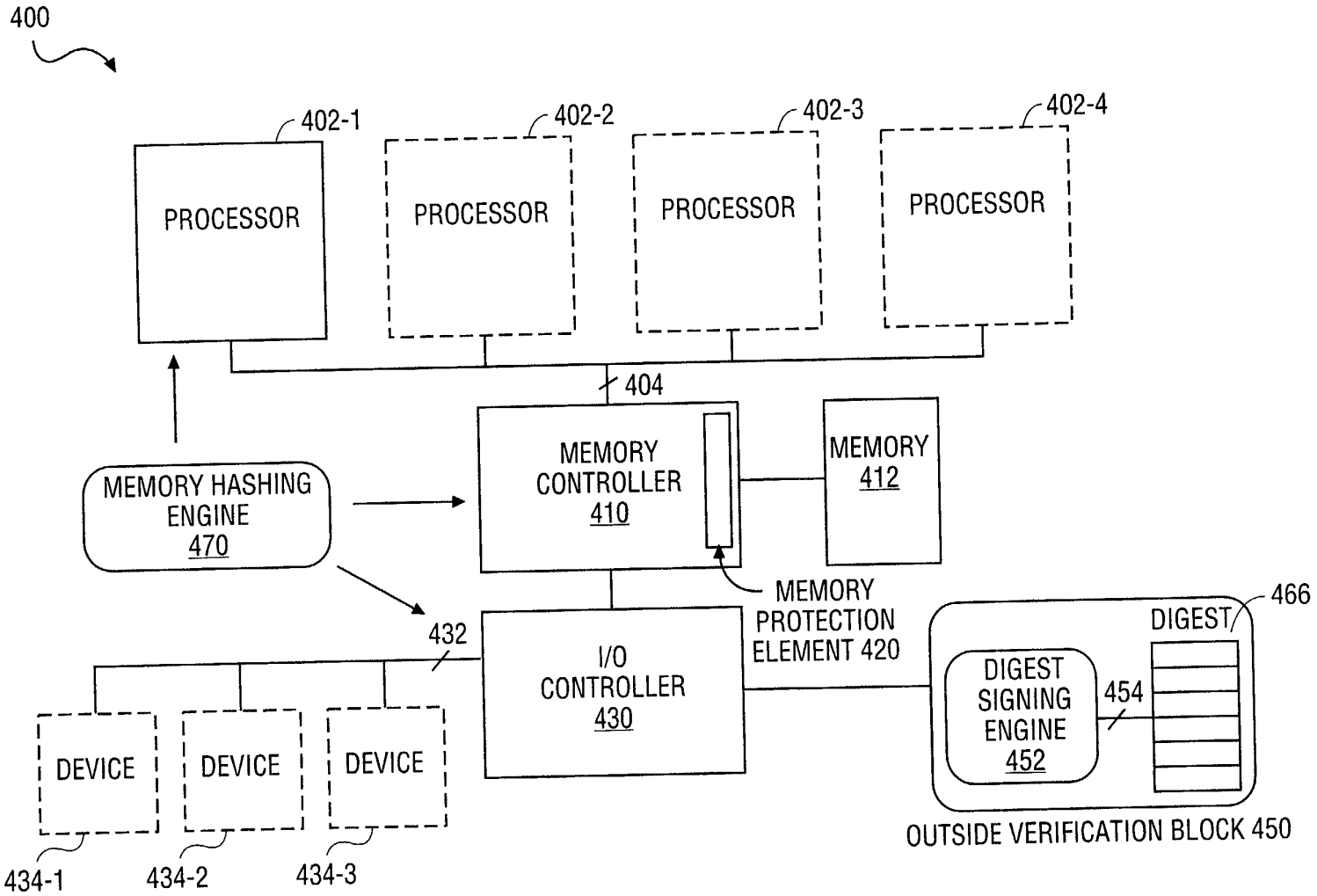

FIG. 4

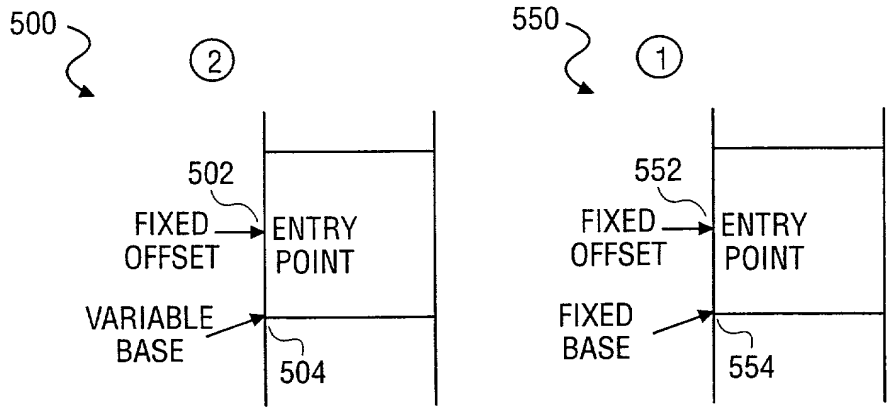
500
2
502
FIXED OFFSET
ENTRY POINT
VARIABLE BASE
504
550
1
552
FIXED OFFSET
ENTRY POINT
FIXED BASE
554
SECURE MEMORY ENVIRONMENTS

FIG. 5A

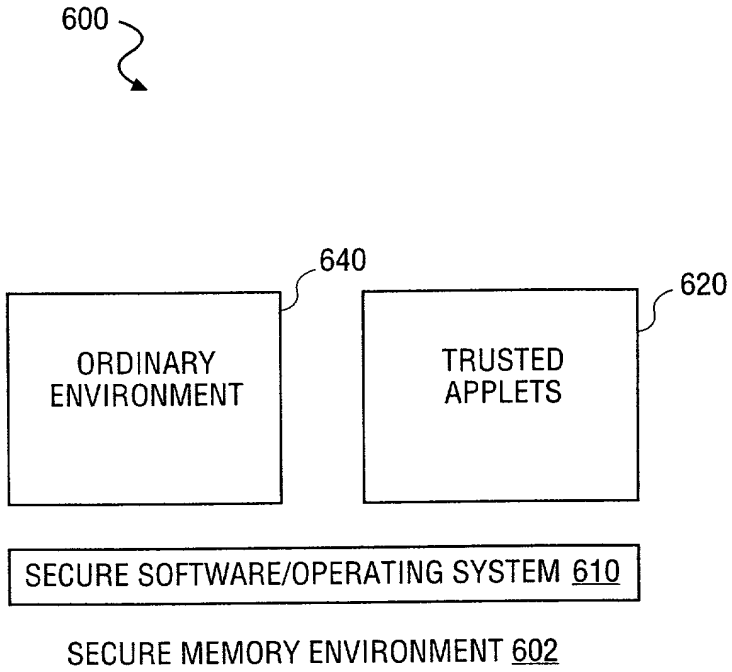
600
640
620
ORDINARY ENVIRONMENT
TRUSTED APPLETS
SECURE SOFTWARE/OPERATING SYSTEM 610
SECURE MEMORY ENVIRONMENT 602

FIG. 5B

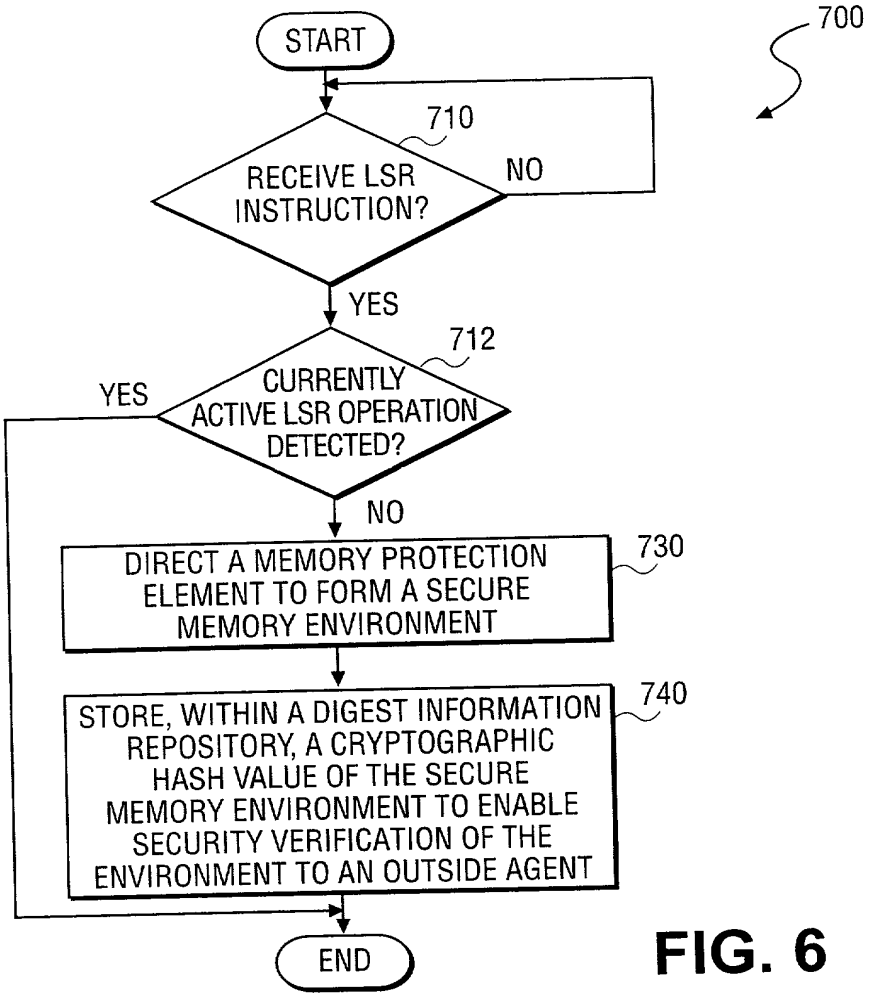
700
START
710
RECEIVE LSR INSTRUCTION?
NO
YES
712
CURRENTLY ACTIVE LSR OPERATION DETECTED?
YES
NO
DIRECT A MEMORY PROTECTION ELEMENT TO FORM A SECURE MEMORY ENVIRONMENT
730
STORE, WITHIN A DIGEST INFORMATION REPOSITORY, A CRYPTOGRAPHIC HASH VALUE OF THE SECURE MEMORY ENVIRONMENT TO ENABLE SECURITY VERIFICATION OF THE ENVIRONMENT TO AN OUTSIDE AGENT
740
END

FIG. 6

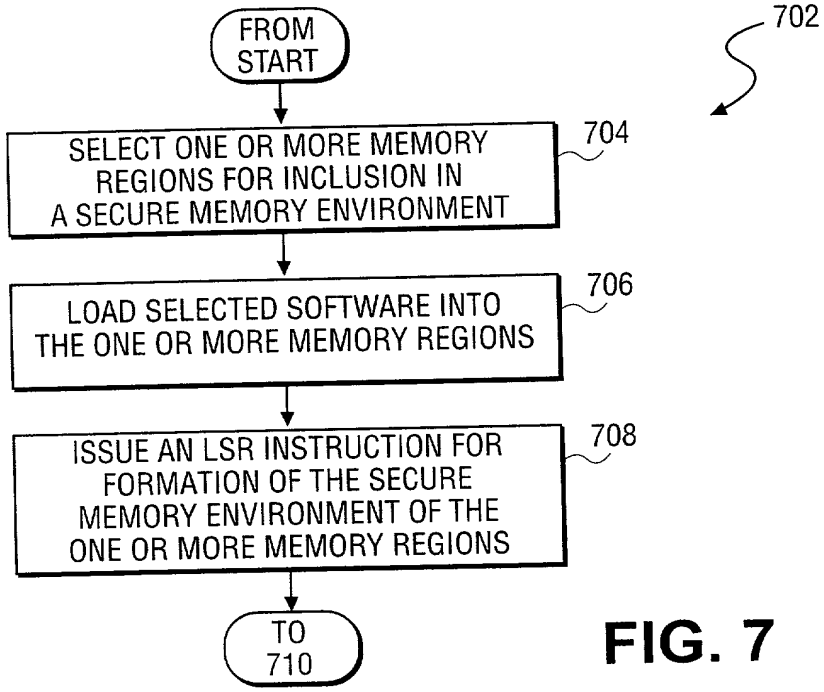
FROM START
702
SELECT ONE OR MORE MEMORY REGIONS FOR INCLUSION IN A SECURE MEMORY ENVIRONMENT
704
LOAD SELECTED SOFTWARE INTO THE ONE OR MORE MEMORY REGIONS
706
ISSUE AN LSR INSTRUCTION FOR FORMATION OF THE SECURE MEMORY ENVIRONMENT OF THE ONE OR MORE MEMORY REGIONS
708
TO 710

FIG. 7

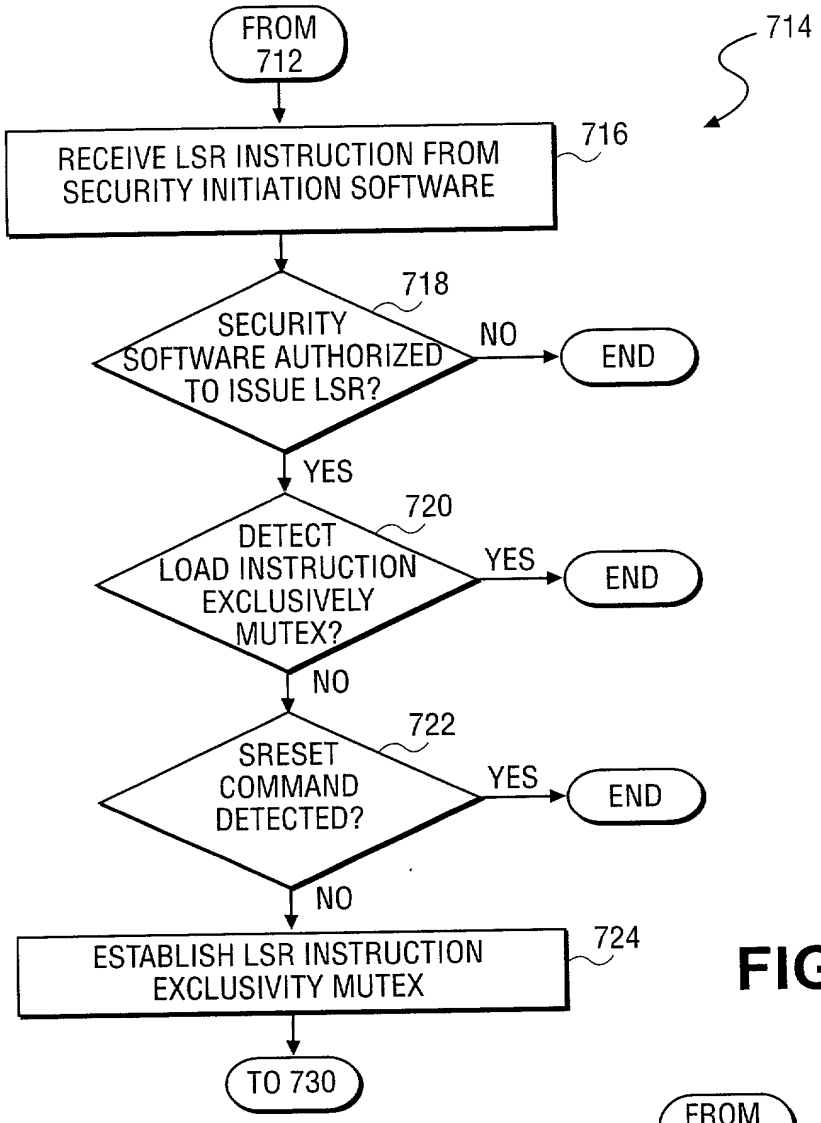
FROM 712
714
RECEIVE LSR INSTRUCTION FROM SECURITY INITIATION SOFTWARE
716
718
SECURITY SOFTWARE AUTHORIZED TO ISSUE LSR?
NO
END
YES
720
DETECT LOAD INSTRUCTION EXCLUSIVELY MUTEX?
YES
END
NO
722
SRESET COMMAND DETECTED?
YES
END
NO
ESTABLISH LSR INSTRUCTION EXCLUSIVITY MUTEX
724
TO 730

FIG. 8

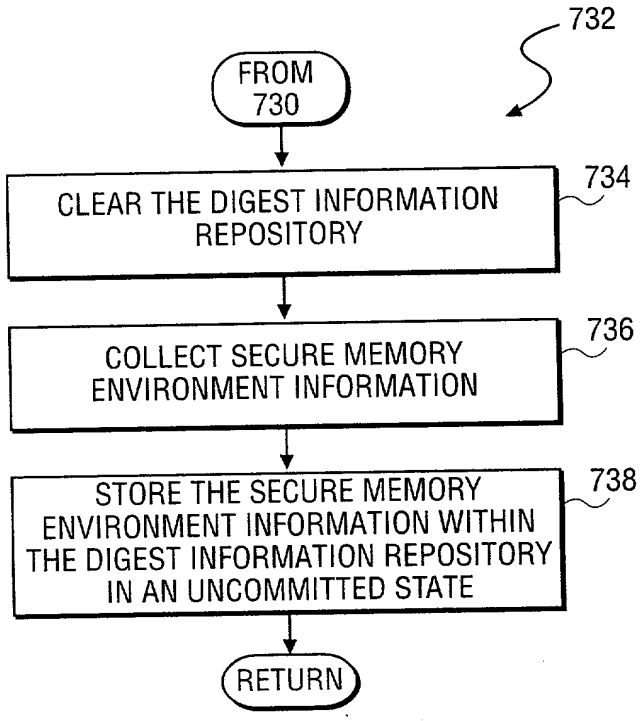
732
FROM 730
CLEAR THE DIGEST INFORMATION REPOSITORY
734
COLLECT SECURE MEMORY ENVIRONMENT INFORMATION
736
STORE THE SECURE MEMORY ENVIRONMENT INFORMATION WITHIN THE DIGEST INFORMATION REPOSITORY IN AN UNCOMMITTED STATE
738
RETURN

FIG. 9

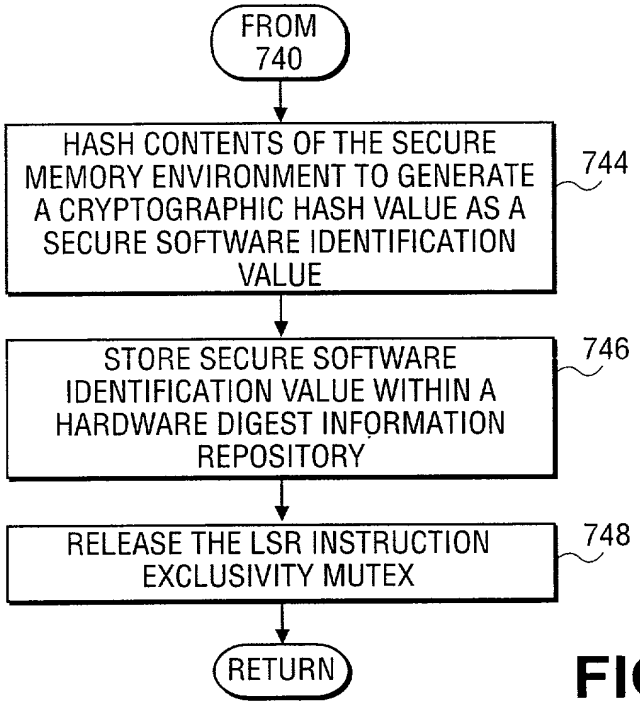
FROM 740
742
HASH CONTENTS OF THE SECURE MEMORY ENVIRONMENT TO GENERATE A CRYPTOGRAPHIC HASH VALUE AS A SECURE SOFTWARE IDENTIFICATION VALUE
744
STORE SECURE SOFTWARE IDENTIFICATION VALUE WITHIN A HARDWARE DIGEST INFORMATION REPOSITORY
746
RELEASE THE LSR INSTRUCTION EXCLUSIVITY MUTEX
748
RETURN

FIG. 10

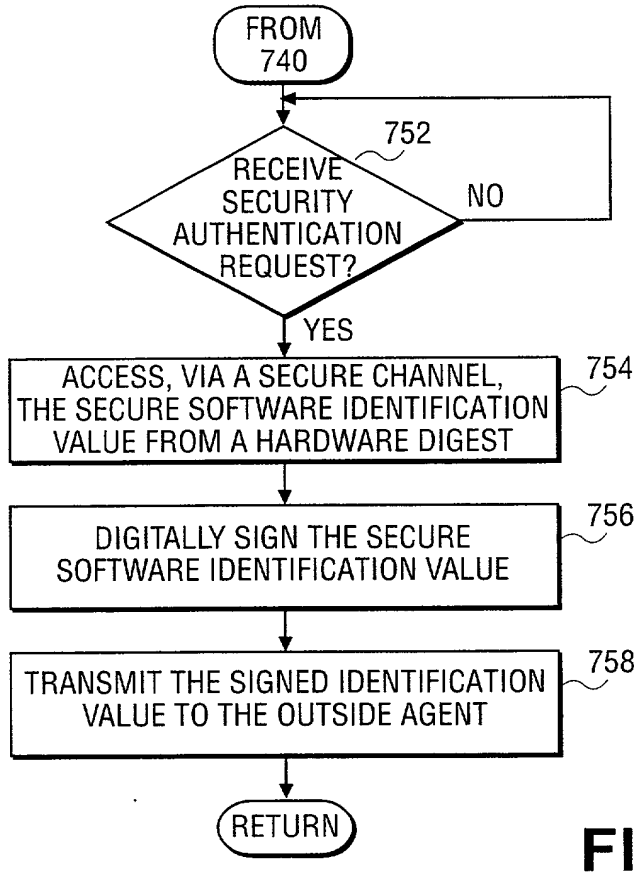
FROM 740
750
752
RECEIVE SECURITY AUTHENTICATION REQUEST?
NO
YES
ACCESS, VIA A SECURE CHANNEL, THE SECURE SOFTWARE IDENTIFICATION VALUE FROM A HARDWARE DIGEST
754
DIGITALLY SIGN THE SECURE SOFTWARE IDENTIFICATION VALUE
756
TRANSMIT THE SIGNED IDENTIFICATION VALUE TO THE OUTSIDE AGENT
758
RETURN

FIG. 11

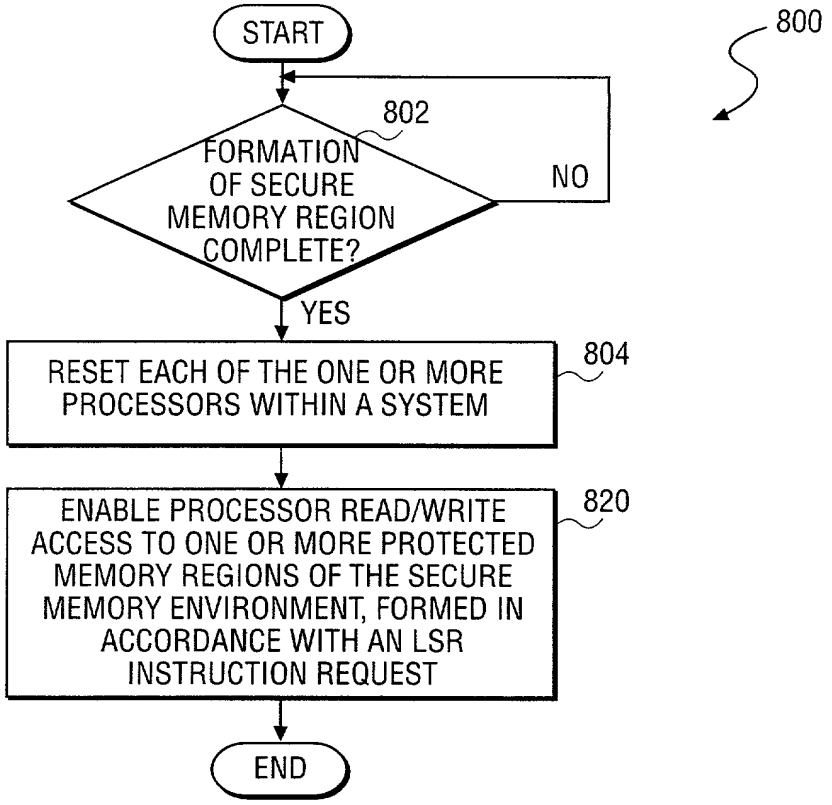
START
800
802
FORMATION OF SECURE MEMORY REGION COMPLETE?
NO
YES
804
RESET EACH OF THE ONE OR MORE PROCESSORS WITHIN A SYSTEM
820
ENABLE PROCESSOR READ/WRITE ACCESS TO ONE OR MORE PROTECTED MEMORY REGIONS OF THE SECURE MEMORY ENVIRONMENT, FORMED IN ACCORDANCE WITH AN LSR INSTRUCTION REQUEST
END

FIG. 12

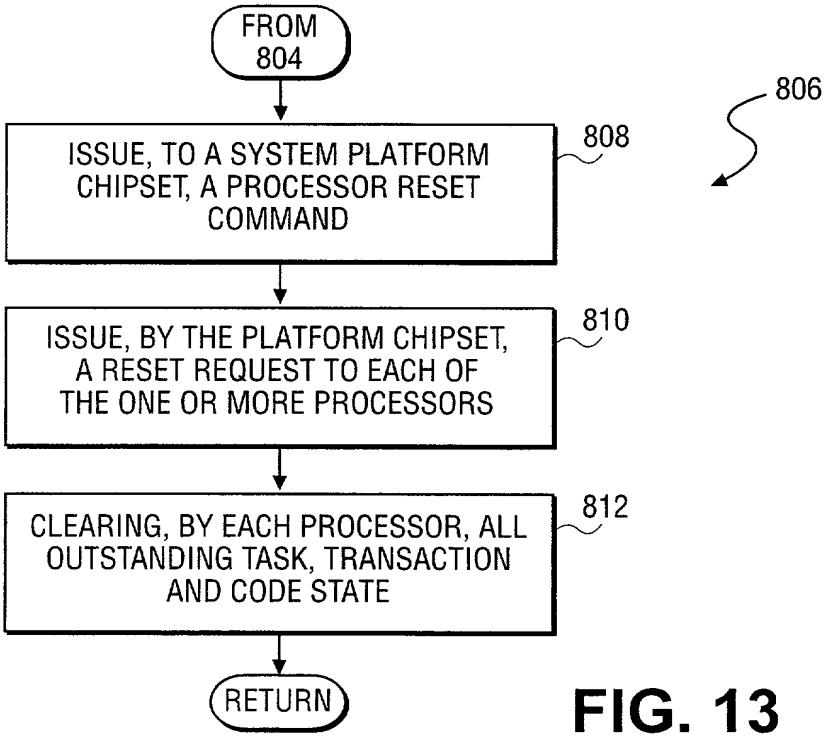
FROM 804
806
808
ISSUE, TO A SYSTEM PLATFORM CHIPSET, A PROCESSOR RESET COMMAND
810
ISSUE, BY THE PLATFORM CHIPSET, A RESET REQUEST TO EACH OF THE ONE OR MORE PROCESSORS
812
CLEARING, BY EACH PROCESSOR, ALL OUTSTANDING TASK, TRANSACTION AND CODE STATE
RETURN

FIG. 13

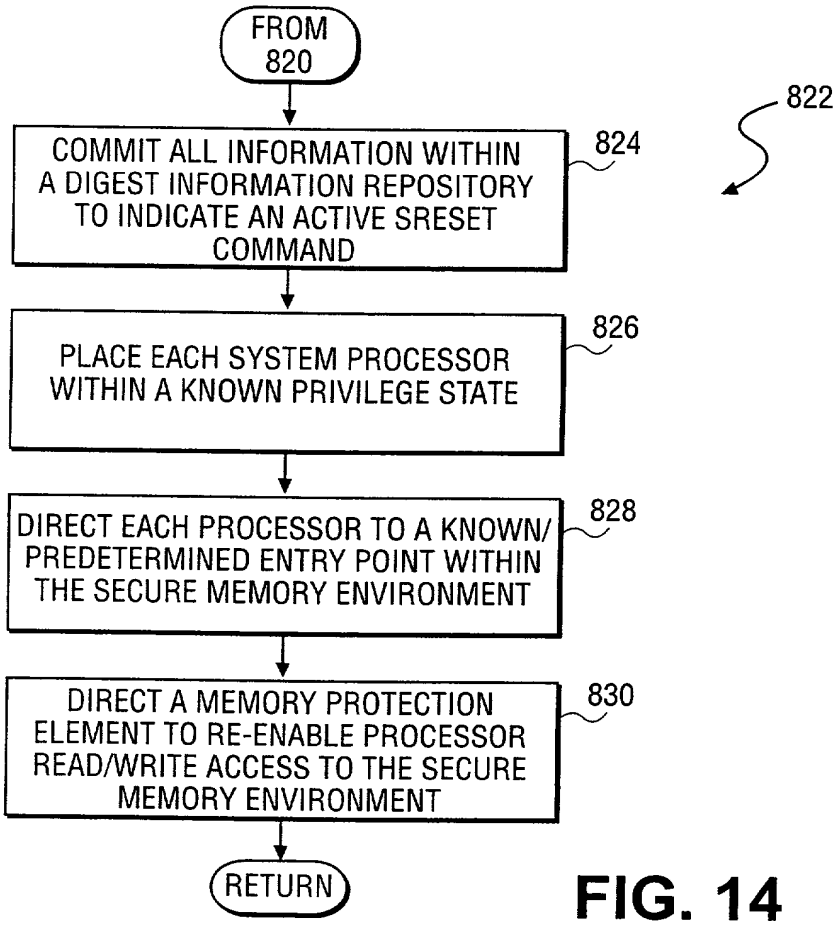
FROM 820
822
COMMIT ALL INFORMATION WITHIN A DIGEST INFORMATION REPOSITORY TO INDICATE AN ACTIVE SRESET COMMAND
824
PLACE EACH SYSTEM PROCESSOR WITHIN A KNOWN PRIVILEGE STATE
826
DIRECT EACH PROCESSOR TO A KNOWN/ PREDETERMINED ENTRY POINT WITHIN THE SECURE MEMORY ENVIRONMENT
828
DIRECT A MEMORY PROTECTION ELEMENT TO RE-ENABLE PROCESSOR READ/WRITE ACCESS TO THE SECURE MEMORY ENVIRONMENT
830
RETURN

FIG. 14